An official website of the United States government Here's how you know

PUBLICATION

Understanding and Responding to Distributed Denial-Of-Service Attacks

Publish Date: March 21, 2024

RELATED TOPICS: CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE, CYBERSECURITY BEST PRACTICES, INCIDENT DETECTION, RESPONSE, AND PREVENTION

This joint guide, Understanding and Responding to Distributed Denial-Of-Service Attacks, addresses the specific needs and challenges faced by organizations in defending against DDoS attacks. The guidance now includes detailed insight into three different types of DDoS techniques:

- Volumetric, attacks aiming to consume available bandwidth.
- Protocol, attacks which exploit vulnerabilities in network protocols.
- Application, attacks targeting vulnerabilities in specific applications or running services.

CISA, FBI, and MS-ISAC urge network defenders and leaders of critical infrastructure organizations to read the guidance provided to defend against this threat. For more actionable recommendations, best practices, and operational insights designed to address common challenges, visit CISA's Capacity Enhancement Guides for Federal Agencies page.

Understanding and Responding to Distributed Denial-of-Service Attacks_508c
(PDF, 1.03 MB)

Tags

Audience: Federal Government, State, Local, Tribal, and Territorial Government

Topics: Critical Infrastructure Security and Resilience, Cybersecurity Best Practices, Incident Detection, Response, and Prevention, Securing Networks, Cyber Threats and Advisories

Related Resources

MAY 24, 2024 ■ PUBLICATION
Cybersecurity Advisory Committee (CSAC) Subcommittee Fact Sheet

MAY 24, 2024 ■ PUBLICATION
Cybersecurity Advisory Committee (CSAC) Reports and Recommendations

MAY 02, 2024
Secure by Design Alert: Eliminating Directory Traversal Vulnerabilities in Software

MAY 01, 2024
Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity